Official Urges Protection Against Identity Theft

Defense Department officials are urging service members to be aware of identity theft and are providing ways for them to protect themselves, the director of DOD's personal finance office said.

Dave Julian noted that officials take the problem very seriously.

"We equate it to service readiness," he said.

Service members dealing with financial issues, he explained, are less likely to be ready to fully perform their missions. Identity theft can cause financial stress, he added.

Young service members who have grown up in the digital world sometimes take a casual approach to divulging information that can be useful to identity thieves, Julian said.

"Our force is part of the digital generation. Our force lives online," he said. "We see that they are very forthcoming with their personal information."

Additionally, he said, members of the military get a steady paycheck, and companies want to show their patriotism by extending credit to them. But that makes it easier for thieves to use service members' stolen identities and profit quickly.

To help service members protect against identity theft, DOD has joined with the Federal Trade Commission on its “Deter, Detect and Defend” campaign, Julian said. While the campaign is aimed at the general public, a brochure has been developed especially for the military.

One of the key suggestions for deploying service members is activating “an active-duty alert,” which requires creditors to obtain specific permission from a service member or an official representative before extending credit. There is no charge for active-duty alerts, he noted, and they last for one year and can be extended.

Active-duty alerts can be activated by calling the toll-free fraud telephone number for one of the three nationwide consumer reporting companies. That company is required to notify the other two companies that a service member has activated a duty alert. Another option service members can use to protect themselves is putting a “freeze” on their credit report to restrict access to it. Once a freeze is in place, potential creditors and other third parties will not be able to get access to a credit report unless the freeze is lifted.

Credit-freeze laws vary from state to state. In some states, only identity-theft victims can freeze their credit. The cost of placing, temporarily lifting or removing a credit freeze also varies. Many states make credit freezes free for identity theft victims, but depending upon where they live, others may pay a fee of typically $10 to each of the three credit-reporting agencies.

Since spouses left at home often handle deployed service members' finances, they should be aware of identity theft and how to protect against it, Julian said, so identity theft usually is covered in pre-deployment briefings that service members and their spouses are encouraged to attend.

Single deployed service members can be at a disadvantage, Julian acknowledged, because they need to watch out for identity theft themselves or have a trusted agent, such as a parent, keep track of their accounts.

But whether single or married, he said, service members who choose to watch their finances while they are deployed need to remember that common-use computers are dangerous things. It's important, he explained, to log off -- completely back out -– if they are monitoring their personal information on a common-use computer or in an Internet café.

Service members should request a copy of their credit report every year from each credit-reporting agency, Julian said. Since there are three credit-reporting agencies, he suggested requesting a different copy from a separate agency every four months.

Identity theft affecting deployed service members is an ongoing problem, said Gary McAlum, senior vice president for enterprise security for USAA, an insurance and financial services company. USAA has worked quickly to lock down the accounts of

known victims and of service members whose information had been stolen but whose accounts had yet to be targeted, he said.

A recent case involved service members victimized by a criminal ring that collected personal information and then used that information to open credit card accounts and drain savings accounts, McAlum said.

Identity thieves sometimes use “social engineering” to obtain information, McAlum said, using an “authoritative-voice” tactic to get someone to offer personal information over the telephone. The thief then uses the same tactic with creditors to get credit. A thief who doesn’t have all of the information required by the creditor, he added, often will “sound dumb” to creditors to obtain the information.

Deploying service members “are obviously not going to be as vigilant as they deploy, get ready to deploy or are coming home from a deployment, so it is important that they use online resources” to make sure everything is in order, said Mike Kelly, USAA spokesman.

McAlum stressed that identity theft is a significant problem for the nation. “The fact that it is exploiting our service members just makes it worse,” he added.

If you discover that your identity has been stolen, call any of the three credit reporting agencies to put a fraud alert on your credit report. Then, order a credit report from each

of the agencies and look for any mistakes or signs of fraud. Also, create an Identity Theft Report by filing a complaint with the FTC and attaching a copy of the police report.

As always, make sure you notify your Commander and First Sergeant ASAP. If you need any additional assistance, the Misawa Legal Office can help.

The three credit reporting agencies can be contacted at:

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-680-7289